REMARKS

The Office Action dated August 2, 2007, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-48 are pending in the application. Claims 1-10, 12-13, 22-43, 46, and 48 are amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 11, 14-21, 44-45, and 47 are canceled. Claims 49-55 are new. No new matter is added. Claims 1-10, 12-13, 22-43, 46, and 48-55 are submitted for consideration in view of the foregoing amendments and the following remarks.

Claims 1-11, 14-17, 19, 20, 22-29, 31, 33-35, 38-39, and 43-48 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings and Peterson (RFC 3325 Internet Draft, http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00, May 27, 2002 – hereinafter Jennings) in view of W. Marshall et al. (draft-ietf-sip-privacy-04.txt, February 27, 2002 – hereinafter Marshall).

The Office Action alleged that Jennings discloses the limitations of a security server receiving a message, determining whether the message has been through a security check, and forwarding the message within a telecommunications network regardless of the result of the determination. However, the Office Action acknowledged that Jennings does not disclose that if the result of the determination is that the message has not been through a security check, modifying the message so as to indicate that the message has not been through a seciruty check. This rejection is traversed as follows.

Claim 1, upon which claims 2-10 and 12-13 depend, is generally directed toward an apparatus that includes a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network and a determiner configured to determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface. The apparatus also includes a forwarder configured to forward the message within the telecommunications network regardless of the result of the determination, and a modifier configured to modify the message so as to indicate that the message has not been through a security check if the result of the determination is that the message has not been through a security check.

Claim 22, upon which claims 23-24 and 49 depend, is generally directed toward a system that includes a security server and a network processing element. The security server is configured to receive a message via a secure interface or directly from outside the system and determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface. The security server is also configured to modify the message so as to indicate that the message has not been through a security check if the result of the determination is that the message has not been through a security check, and to forward the message to the network processing element regardless of the result of the determination.

Claim 25, upon which claim 50 depends, generally discloses a method that includes receiving a message via a secure interface or directly from outside a

telecommunications network and determining that the message has not been through a security check by determining that it has not been received via the secure interface. The method also includes modifying the message so as to indicate that the message has not been through a security check and forwarding the message within the telecommunications network.

Claim 26, upon which claims 27-32 and 51 depend, is generally directed toward an apparatus that includes a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network and a determiner configured to determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface. The apparatus also includes a forwarder configured to forward the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check.

Claim 33, upon which claims 34-42 and 52 depend, is generally directed toward a system that includes a security server and a network processing element. The security server is configured to receive a message via a secure interface or directly from outside the system and determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface. The security system is also configured to forward the message to the network processing

element regardless of the result of the determination, but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check.

Claim 43, upon which claim 53 depends, is generally directed to a method that includes receiving a message via a secure interface or directly from outside a telecommunications network, determining that the message has not been through a security check by determining that the message has not been received via the secure interface, and forwarding the message within the communications network in a manner that indicates that the message has not been through a security check.

Claim 46, upon which claim 54 depends, is generally directed to an apparatus that includes a receiving means for receiving a message via a secure interface or directly from outside a telecommunications network and a determining means for determining whether the message has been through a security check by determining whether or not the message has been received via the secure interface. The apparatus also includes a modifying means for, if the message is determined not to have been through a security check, modifying the message to indicate that it has not been through a security_check, and a forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check.

Claim 48, upon which claim 55 depends, is generally directed to an apparatus that includes a receiving means for receiving a message via a secure interface or directly from

outside a telecommunications network and a determining means for determining whether the message has been through a security check by determining whether or not the message has been received via the secure interface. The apparatus also includes a forwarding means for forwarding the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forwarding the message in a manner that indicates that the message has not been through a security check.

Each of the foregoing independent claims recites limitations that are not disclosed or suggested by a combination of Jennings and Marshall.

Jennings generally discloses private extension to session initiation protocol (SIP) that enable a network of trusted SIP servers to assert the identity of end users or end systems, and the application of existing privacy mechanisms. In Jennings, the use of the extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport and usage of such information.

Marshall generally discloses extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy. Marshall discloses that the use of these extensions are only applicable inside an administrative domain, or among federations of administrative domains with previously agreed-upon policies for usage of such information.

However, a combination of Jennings and Marshall fails to disclose or suggest all the limitations of the pending claims. As presented above, each of the independent

claims currently includes limitations analogous to those previously presented in claims 11 and 12 (where claim 12 depended from claim 11). For example, claim 1 now includes "a receiver configured to receive a message v*ia a secure interface or directly from outside a telecommunications network* [and] a determiner configured to determine whether the message has been through a security check *by determining whether or not the message has been received via the secure interface*." [emphasis added]. These limitations are neither disclosed nor suggested by a combination of Jennings and Marshall.

Regarding claims 12, the Office Action acknowledged that Jennings and Marshall fail to disclose or suggest a Za interface. As presented above, claim 1, analogous to the Za interface of claim 12, recites receiving a message via a "secure interface" or "directly from outside a telecommunications network." Additionally, not only does claim 1 recite a "secure interface," but also discloses operations based upon the secure interface including determining "whether the message has been sent through a security check by determining whether or not the message has been received via the secure interface." Accordingly, a combination of Jennings and Marshall fails to disclose or suggest each limitation of claim 1 as required by a proper §103(a) rejection.

Therefore, Applicants respectfully request that the rejection of claim 1 be withdrawn. Similarly, Applicants request that the rejection of claims 22, 25, 26, 33, and 43 be withdrawn for reciting limitations similar to the limitations of claim 1, though each claim has its own scope. Furthermore, Applicants request that the rejection of claims 2-

10, 23-24, 27-29, 31, 34-35, and 38-39, be withdrawn for at least their dependency from claims 1, 22, 25, 26, and 33.

Claims 12, 30, 37, and 41 were rejected under 35 U.S.C. §103(a) as unpatentable over Jennings in view of Marshall as applied to claims 1, 28, 33, and 39 above, and further in view of Arkko et al. (US 2002/0052200 A1 – hereinafter Arkko). As mentioned above, the Office Action acknowledged that Jennings and Marshall do not disclose a secure means such as a ZA (i.e., a secure interface). To support the rejection, the Office Action cites to Arkko as disclosing a secure means such as a Za interface. This rejection is traversed as follows.

As provided above, Jennings and Marshall fail to disclose or suggest "a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network [and] a determiner configured to determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface," as recited in claim 1. Similarly, Arkko fails to disclose these limitations.

Arkko generally discloses an encrypted mobile application part protocol message that is sent between a first network element of a first telecommunications network and a second network element of a second telecommunications network.

However, Arkko fails to disclose or suggest "a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network [and] a determiner configured to determine whether the message has been through a

security check by determining whether or not the message has been received via the secure interface."

Instead, Arkko discloses that the first network element uses a master security association to derive a connection-specific security association, and includes in the encrypted mobile application part message a parameter obtained from the connection specific security association. Upon receipt at the second network element, the master security association is used to drive a connection-specific security association for use by the second network element. The second network element uses the connection-specific security association to decrypt the mobile application part message.

In support of the §103(a) rejection, the Office Action cites to Arkko at paragraphs [0040] – [0043] and Figures 1 and 2. However, these passages fail to provide for "a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network [and] a determiner configured to determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface."

For example, paragraph [0040], in combination with Figure 4, presents a key management architecture that includes Za, Zb, and Zc interfaces. Paragraphs [0041] – [0043] disclose contexts for the Za, Zb, and Zc interfaces, respectively. Additionally, Figures 1 and 2, depict Za, Zb, and Zc interfaces. However, none of these Figures or paragraphs disclose or suggest using a "secure interface" (i.e., a Za interface) as a basis for judging whether or not a message has been through a security check. In other words,

Arkko fails to provide for the logical instructions, circuits, and/or devices for using the Za interface in a manner that provides for the limitations of claim 1.

Accordingly, a combination of Jennings, Marshall, and Arkko fails to disclose or suggest each limitation of claim 1, from which claim 12 depends. Similarly, a combination of Jennings, Marshall, and Arkko fails to disclose or suggest the limitations of claim 30, 37, and 41 which depend from claims 26, 33, and 33. Therefore, Applicants respectfully request that the rejection of claims 12, 30, 37, and 41 be withdrawn.

Claims 13, 21, 32, and 42 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Marshall as applied to claims 1, 14, and 33, and further in view of Soininen (RFC 3574 Internet Draft, http://tols.ietf.org/html/draft-ietf-v6ops-3gpp-cases-00, September, 2002 – hereinafter Soininen). The Office Action acknowledged that Jennings and Marshall do not dislcose where the security server including an interrogating call session control function, but relied upon Soininen to provide for this limitation. This rejection is traversed as follows.

As presented above, a combination of Jennings and Marshall fails to disclose or suggest each limitation of claims 1, 26, and 33, from which claims 13, 32, and 43 depend. Similarly, a combination of Jennings, Marshall, and Soininen fails to disclose all the limitations of claims 1, 26, and 33 because Soininen fails to account for the deficiencies of Jennings and Marshal.

Soininen generally discloses different scenarios in a Third Generation Partnership Project (3GPP) defined packet network that would need IP versions 6 and IP version 4

transitions. However, Soininen fails to disclose or suggest, at least, "a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network [and] a determiner configured to determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface," as recited in claim 1. Instead, Soininen discloses scenarios where the user equipment connects to nodes in other networks, e.g., the Internet. Indeed, Soininen is silent with respect to determining whether a message has been sent through a security check based on whether the message has been received via a secure interface.

Accordingly, a combination of Jennings, Marshall, and Soininen fails to disclose or suggest all the limitations of claims 1, 26, and 33, from which claims 13, 32, and 43 depend. Therefore, Applicants respectfully request that the rejection of claims 13, 32, and 43 be withdrawn.

Claims 18-20 were rejected under 35 U.S.C. §103(a). However, this rejection is moot in light of the cancellation of claims corresponding thereto.

Claims 36 and 40 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Marshall as applied to claim 35, further in view of Haukka (US 2003/0210678 A1 – hereinafter Haukka). The Office Action acknowledged that Jennings and Marshal do not disclose where the internal security system comprises a UMTS specified security system, but relied on Haukka to disclose the internal security system comprising a UMTS specified security system. This rejection is traversed as follows.

As presented above, a combination of Jennings and Marshall fails to disclose or suggest all the limitations of claim 33, from which claims 36 and 40 depend. Simialrly, a combination of Jennings, Marshall, and Haukka fails to disclose or suggest all the limitations of claim 33 because Haukka fails to account for the deficiencies of Jennings and Marshall.

Haukka generally discloses a method and apparatus for connecting terminal equipment to a wireless network with a mobile terminal, where the mobile terminal is assigned proxy functions that control access of the terminal equipment to an internet protocol multimedia subsystem (IMS) in the wireless network.

However, Haukka fails to disclose or suggest, at least, "the security server being configured to receive a message via a secure interface or directly from outside the system, determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface," as recited in claim 33, from which claims 36 and 40 depend.

Instead, Haukka discloses that terminal equipment perform protocol stream processing functions for communicating with the IMS. The protocol stream processing functions include real-time transport protocol (RTP) and real-time transport control protocol (RTCP) functions. The wireless network includes a universal mobile telecommunications system (UMTS) network coupled to the internet protocol multimedia subsystem (IMS). The internet protocol multimedia subsystem (IMS) includes a session

initiation protocol (SIP) server for providing internet protocol multimedia information signals.

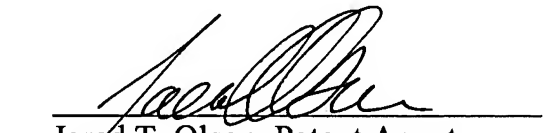
Accordingly, a combination of Jennings, Marshall, and Haukka fails to disclose or suggest all the limitations of claim 33, from which claims 36 and 40 depend, as required by a proper §103(a) rejection. Therefore, Applicants respectfully request that the §103(a) rejection of claims 36 and 40 be withdrawn for at least their dependency from claim 33.

In light of the foregoing, the cited references fail to disclose or suggest all the limitations of any of the pending claims. Accordingly, Applicants respectfully request that the rejections of the pending claims be withdrawn. Furthermore, Applicants request that claims 1-10, 12-13, 22-43, 46, and 48-55 pass to issue and allowance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Jared T. Olson, Patent Agent
Registration No. 61,058

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

Enclosures: Petition for Extension of Time